Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: September 25, 2025
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/essehealth

June 25, 2025

Notice of Data <<Variable Text 2: Security Incident/Breach>>

Dear <<First Name>> <<Last Name>>,

Esse Health was recently impacted by a cyber event that affected the security of some files stored in our computer system. We are notifying you because some information related to you may have been contained within those files.

What Happened

On April 21, 2025, suspicious activity was identified within the Esse Health network. Upon learning of this activity, we initiated an investigation with the assistance of external cybersecurity and forensic specialists. Based on the investigation, a cybercriminal gained access to our network on April 21, 2025. While in our network, the cybercriminal was able to view and copy certain files. As part of our investigation, we conducted a time-intensive review of the files involved to determine the types of data present and to whom it related. This review identified that information related to you may have been contained in those files.

What Information Was Involved

The data involved varied by individual, but may have included information such as name, address, date of birth, health insurance information, medical record number, patient account number, and certain health information. There is no indication that your social security number was involved. It is also important to note that NextGen, our electronic medical record system was not accessed or copied.

What We Are Doing

We take the privacy and security of your information seriously. Upon learning of this event, we promptly took steps to secure our systems and respond to this event. We also notified law enforcement. As part of our ongoing commitment to the privacy and security of information in our care, we have implemented additional security enhancements to further strengthen our defenses. Although at this time there is no indication that any of the involved information has been misused, as an added precaution, we are offering you identity protection services at no charge through IDX, a data breach and recovery services provider.

What You Can Do

We invite you to enroll in the free identity protection services by calling 1-855-202-3424 or going to https://response.idx.us/essehealth. You will find detailed instructions for enrollment on the enclosed **Additional Steps** document. Also, you will need to reference the Enrollment Code at the top of this letter when calling or enrolling online,

so please do not discard this letter. Please note the deadline to enroll is September 25, 2025. In addition, as a precaution, it is always good practice to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Additional information about the steps you can take is contained in the enclosed **Additional Steps** document.

For More Information

If you have any questions or would like additional information please call the dedicated call center we set up to help answer your questions regarding this incident at 1-855-202-3424 Monday through Friday from 8 am - 8 pm Central Time or go to https://response.idx.us/essehealth. You may also write to us at inquiries@essehealth.com.

At Esse Health, our patients are our highest priority. We apologize for any inconvenience this caused and would like to thank you for your continued partnership.

Sincerely,

Jaime L. Bremerkamp, FACHE
Privacy Officer, Esse Health

(Enclosure)

Additional Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://response.idx.us/essehealth and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-855-202-3424 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports for unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies listed below, whether or not you suspect any authorized activity on your account. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about fraud alerts, security freezes, and steps you can take toward preventing identity theft from the three major credit reporting companies listed above and the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To the Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: September 25, 2025
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/essehealth

June 25, 2025

Notice of Data <<Variable Text 2: Security Incident/Breach>>

Dear Parent or Guardian of <<First Name>> <<Last Name>>,

Esse Health was recently impacted by a cyber event that affected the security of some files stored in our computer system. We are notifying you because some information related to your child may have been contained within those files.

What Happened

On April 21, 2025, suspicious activity was identified within the Esse Health network. Upon learning of this activity, we initiated an investigation with the assistance of external cybersecurity and forensic specialists. Based on the investigation, a cybercriminal gained access to our network on April 21, 2025. While in our network, the cybercriminal was able to view and copy certain files. As part of our investigation, we conducted a time-intensive review of the files involved to determine the types of data present and to whom it related. This review identified that information related to your child may have been contained in those files.

What Information Was Involved

The data involved varied by individual, but may have included information such as name, address, date of birth, <<Variable Text 1>>. <<Variable Text 3>>. It is important to note that NextGen, our electronic medical record system was not accessed or copied.

What We Are Doing

We take the privacy and security of your information seriously. Upon learning of this event, we promptly took steps to secure our systems and respond to this event. We also notified law enforcement. As part of our ongoing commitment to the privacy and security of information in our care, we have implemented additional security enhancements to further strengthen our defenses. Although at this time there is no indication that any of the involved information has been misused, as an added precaution, we are offering you identity protection services at no charge through IDX, a data breach and recovery services provider.

What You Can Do

We invite you to enroll in the free identity protection services on behalf of your child by calling 1-855-202-3424 or going to https://response.idx.us/essehealth. You will find detailed instructions for enrollment on the enclosed **Additional Steps** document. Also, you will need to reference the Enrollment Code at the top of this letter when calling

or enrolling online, so please do not discard this letter. Please note the deadline to enroll is September 25, 2025. Additional information about the steps you can take is contained in the enclosed **Additional Steps** document.

For More Information

If you have any questions or would like additional information please call the dedicated call center we set up to help answer your questions regarding this incident at 1-855-202-3424 Monday through Friday from 8 am - 8 pm Central Time or go to https://response.idx.us/essehealth. You may also write to us at inquiries@essehealth.com.

At Esse Health, our patients are our highest priority. We apologize for any inconvenience this caused and would like to thank you for your continued partnership.

Sincerely,

Jaime L. Bremerkamp, FACHE
Privacy Officer, Esse Health

(Enclosure)

Additional Steps to Help Protect Your Child's Information

1. **Website and Enrollment.** Go to https://response.idx.us/essehealth and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Telephone. Contact IDX at 1-855-202-3424 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your child's credit identity.

3. Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Security Freeze. You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your child's credit files.

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable

information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: September 25, 2025
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/essehealth

June 25, 2025

Notice of Data <<Variable Text 2: Security Incident/Breach>>

Dear <<First Name>> <<Last Name>>,

Esse Health was recently impacted by a cyber event that affected the security of some files stored in our computer system. We are notifying you because some information related to you may have been contained within those files.

What Happened

On April 21, 2025, suspicious activity was identified within the Esse Health network. Upon learning of this activity, we initiated an investigation with the assistance of external cybersecurity and forensic specialists. Based on the investigation, a cybercriminal gained access to our network on April 21, 2025. While in our network, the cybercriminal was able to view and copy certain files. As part of our investigation, we conducted a time-intensive review of the files involved to determine the types of data present and to whom it related. This review identified that information related to you may have been contained in those files.

What Information Was Involved

The data involved varied by individual, but may have included information such as name, address, date of birth, health insurance information, social security number, and certain health information such as vaccination status.

What We Are Doing

We take the privacy and security of your information seriously. Upon learning of this event, we promptly took steps to secure our systems and respond to this event. We also notified law enforcement. As part of our ongoing commitment to the privacy and security of information in our care, we have implemented additional security enhancements to further strengthen our defenses. Although at this time there is no indication that any of the involved information has been misused, as an added precaution, we are offering you identity protection services at no charge through IDX, a data breach and recovery services provider.

What You Can Do

We invite you to enroll in the free identity protection services by calling 1-855-202-3424 or going to https://response.idx.us/essehealth. You will find detailed instructions for enrollment on the enclosed **Additional Steps** document. Also, you will need to reference the Enrollment Code at the top of this letter when calling or enrolling online, so please do not discard this letter. Please note the deadline to enroll is September 25, 2025. In addition, as a precaution,

it is always good practice to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Additional information about the steps you can take is contained in the enclosed **Additional Steps** document.

For More Information

If you have any questions or would like additional information please call the dedicated call center we set up to help answer your questions regarding this incident at 1-855-202-3424 Monday through Friday from 8 am - 8 pm Central Time or go to https://response.idx.us/essehealth. You may also write to us at inquiries@essehealth.com.

We apologize for any inconvenience this caused and would like to thank you for your continued partnership.

Sincerely,

Jaime L. Bremerkamp, FACHE
Privacy Officer, Esse Health

(Enclosure)

Additional Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://response.idx.us/essehealth and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-855-202-3424 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports for unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies listed below, whether or not you suspect any authorized activity on your account. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about fraud alerts, security freezes, and steps you can take toward preventing identity theft from the three major credit reporting companies listed above and the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.